What is claimed is:

1. A method for image tamper detection, comprising the steps of:

(a) computing a thumbnail of an original image;

(b) embedding the computed thumbnail in the original image to create a marked image;

(c) transmitting the marked image to a recipient;

(d) extracting the embedded thumbnail from the transmitted marked image;

(e) computing a new thumbnail of the received image;

(f) differencing the extracted thumbnail from the new thumbnail to create a difference image that represents the similarity of the two thumbnails;

(g) alerting if the difference image shows the two thumbnails are not sufficiently similar; and

(h) authenticating the image if the difference image shows the two thumbnails are sufficiently similar.

2. A method for image tamper detection according to claim 1, wherein step (b) includes ensuring that the embedding does not change the size of the original image.

3. A method for image tamper detection according to claim 1, wherein step (b) includes ensuring that the embedding does not change the dynamic range of the original image.

4. A method for image tamper detection according to claim 1, wherein step (b) further comprises employing a data hiding technique that is resistant to channel noise.

5. A method for image tamper detection according to claim 1, wherein step (b) further comprises employing a data hiding technique that is resistant to image compression.

6. A method for image tamper detection according to claim 5, wherein the image compression technique is JPEG.

7. A method for image tamper detection according to claim 5, wherein step (b) further comprises employing a data hiding technique that is resistant to channel noise.

8. A method for image tamper detection according to claim 1, wherein step (b) further comprises employing a data hiding technique based on Spread Spectrum Image Stenography.

9. A method for image tamper detection according to claim 1, wherein said thumbnail is defined as a low resolution version of an image.

10. A method for image tamper detection according to claim 1, wherein steps (a) and (e) further comprise employing a wavelet decomposition.

11. A method for image tamper detection according to claim 1, wherein step (g) further comprises threshholding the difference image to provide automatic detection of tampering.

12. An apparatus for image tamper detection that creates and authenticates marked images based on thumbnail processing of that image, said apparatus comprising:

(a) a memory having instructions stored therein, said instructions being executable to perform a process of thumbnail computation; and

(b) a processor comprising means for executing said instructions, said instruction comprising the operations of:

(i) accepting an original image or a marked image;

(ii) performing thumbnail processing of the accepted image

to:

a. derive a thumbnail of the accepted image,

b. create a marked image from the accepted original image and said derived thumbnail, and

c. authenticate an accepted marked image with said derived thumbnail.

13. The apparatus of claim 12, wherein said marked image is created by embedding said derived thumbnail in the accepted image.

14. The apparatus of claim 12, wherein said operation (ii)(3) includes extracting an embedded thumbnail from the accepted marked image and comparing said derived thumbnail with said embedded thumbnail for similarity.

15. A system for image tamper detection that creates and authenticates marked images based on thumbnail processing of that image, said system comprising:

(a) means for computing a thumbnail;

(b) means for marking an original image with said thumbnail; and

(c) means for authenticating a marked image with said thumbnail.

16. A medium that stores instructions for image tamper detection that creates and authenticates marked images based on thumbnail processing of that image, adapted to be executed by at least one processor to perform the steps of:

(a) accepting an original or marked image;

(b) computing a derived thumbnail from the accepted image;

(c) for an accepted original image, embedding the derived thumbnail into the accepted image;

(d) for an accepted marked image, extracting an embedded thumbnail from the marked image; and

(e) for an accepted marked image, comparing said derived thumbnail with said extracted thumbnail to determine similarity.